REMARKS

Claims 1-18, 20-29, and 32 are pending and at issue. Of these, claims 1, 11, 18, 20, and 29 are independent. Claims 19, 30, and 31 were previously canceled. By this amendment, claim 1 is amended to make a minor grammatical change to the claim. This amendment to claim 1 does not change the scope of claim 1 and is not made for patentability purposes.

This amendment is timely filed as it is submitted on May 24, 2005 with a certificate of mailing under 37 C.F.R. §1.8, a petition for a one-month extension of time, and an authorization to charge the $120.00 for the required petition fee under 37 C.F.R. §1.17(a)(1) to the undersigned attorney's deposit account, thereby extending the response date to May 24, 2005. Although applicants believe that no other fees are due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 13-2855 of Marshall, Gerstein & Borun LLP. In addition, if a petition for any additional extension of time under 37 C.F.R. 1.136(a) is necessary to maintain the pendancy of this case and is not otherwise requested in this case, applicants request that the Commissioner consider this paper to be a petition for an appropriate extension of time and hereby authorize the Commissioner to charge the fee as set forth in 37 CFR 1.17(a) corresponding to the needed extension of time to Deposit Account No. 13-2855 of Marshall, Gerstein & Borun LLP.

Applicants respectfully traverse the rejection of claims 1-18, 20-29, and 32 as anticipated by He et al., U.S. Patent No. 6,088,451 ("He et al."). Each of the pending claims recites a system or a method wherein security information is collected from a user contemporaneously with the initiation of a function implemented within a process control system and wherein the execution of the function is determined based on the

contemporaneously collected security information. He et al. fails to disclose the collection of security information from a user contemporaneously with the initiation of a function to determine whether the function may be executed within any type of system, much less within a process control system. As a result, He et al. cannot anticipate any of the pending claims.

Generally speaking, He et al. discloses a system for use in a computer implemented communications network that protects against unauthorized network machines attempting to impersonate a validly authenticated network machine to obtain information stored in a database associated with the network. However, He et al. does not disclose the collection of security information ***from a user contemporaneously*** with the initiation of a function to determine whether the function may be executed. Instead, similar to other known systems, the He et al. system collects security information from a user only once during an initial login process (before the initiation of a function) and thereafter uses that security information in performing database access operations.

More particularly, He et al. discloses a security server that receives a user login ID from a network user element, e.g., a user workstation, and that then issues an encrypted session ticket to the user machine based on that user login procedure. The session ticket is decrypted by the user machine using a user password collected during the login process. Thereafter, any subsequent communication between the user machine and the server or other network element requires passing the decrypted session ticket. However, He et al. specifically discloses that, once the session ticket is decrypted by the user machine during the login process, no further authentication input is required from the user. In fact, He et al. specifically states that "[t]he NSS 208 [the security server]... generates a general ticket to be used by the user element for future network access requests. After ID and password

authentication has been completed, the general ticket is encrypted using a secret key assigned by, and only know[n] to, the NSS 208 so that future access requests by the same user element can be quickly authenticated by the NSS 208. ***This avoids the NSS 208 having to verify the ID and password each time the user element makes an access request.***" Col. 27 lines 23-31 (emphasis added).

Thus, after the first time the user logs in to a particular user machine within the He et al. system, the user machine may be used to access a server or network element without any further collection of security information from the user. Unlike the method and device of the pending claims, He et al. does not disclose collecting security information from the user contemporaneously with the initiation of a function. Instead, He et al. is similar to other known systems which first collect user security information at a login stage (before a user tries to initiate a function) and which then use this previously collected information whenever any user tries to initiate an operation within the system from the machine on which the login procedure occurred to verify the authorization for that operation. In other words, He et al. does not disclose the collection of security information from the user contemporaneously with the initiation of a function for determining whether the function may be executed, as recited by the pending claims, but instead discloses using previously collected (and stored) security information upon the initiation of a function.

Applicants respectfully disagree with the examiner's contention that column 9, lines 47-61 of the He et al. patent discloses the collection of security information from a user contemporaneously with the initiation of a function. While column 9, lines 47-61 of He et al. generally states that "[u]ser access authorization and control must be performed for each and every individual user request to access network resources and information," this passage of

He et al. does not state or suggest that the user access authorization information can or should be collected contemporaneously from the user at the time that the "user request" is initiated. Instead, and as discussed above, the system described with a high degree of particularity in the rest of the He et al. patent makes it clear that, within the He et al. system, the "user authorization and control" for "every individual user request to access network resources" is implemented by collecting security information from a user as part of an initial login procedure, generating a session ticket based on that security information and then using that session ticket when implementing any subsequently requested operations. Basically, this passage of He et al. merely states (in a general manner) that the He et al. system uses user security information upon the initiation of each operation, but fails to state that the He et al. system obtains this user security information from the user contemporaneously with the initiation of a function, as is recited by the pending claims.

As a result, the He et al. system, similar to other known systems, contains a security loophole because, after a user logs on to a user terminal, thereby completing the general system authentication procedure, any other person may use that same user terminal to access functions enabled by the login procedure. The system and method of the pending claims, on the other hand, prevent unauthorized execution of critical functions by requiring collection of security information from the user contemporaneously with the initiation of a function and using the contemporaneously collected security information to determine whether the function may be executed. This procedure assures that the user who is actually requesting a function is authorized to do so (not merely that a previously authorized terminal is being used to request a function). Consequently, using the claimed system, process critical functions may be protected against unauthorized execution even after a general terminal authentication

process has been performed by an authorized user. Because He et al. discloses an automated login process that uses a single collection procedure for the collection of authentication/authorization information for general access to the system at a user terminal, He et al. does not disclose the collection of security information from a user contemporaneously with the initiation of a function, as recited by the pending claims.

Moreover, He et al. does not teach, in any manner, a security system that is used in a process control system or to perform process control functions, as recited by the pending claims. Instead, He et al. merely discloses a communications security system that involves a user element and a network element that may include "switches signaling transfer points (STPs), data access points (DAPs), mainframe computers, etc." He et al. simply fails to disclose or suggest that its security system may be applied to process control system devices, much less to perform functions on process control system devices.

Because He et al. fails to disclose the collection of security information from a user contemporaneously with the initiation of a function to determine whether the function may be executed, as recited by each of the pending claims, or the use of a security system in a process control system, it follows that He et al. can not anticipate any of the pending claims.

Still further, it is clear that the prior art must make a suggestion of or provide an incentive for a claimed combination of elements to establish a *prima facie* case of obviousness. *See, In re Oetiker*, 24 U.S.P.Q.2d 1443, 1446 (Fed. Cir. 1992); *Ex parte Clapp*, 227 U.S.P.Q. 972, 973 (Bd. Pat. App. 1985). This principle holds true even if the applied art could be modified to produce the invention recited by the pending claims. *See, In re Mills,* 16 U.S.P.Q.2d 1430, 1432 (Fed. Cir. 1990); *In re Gordon,* 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984) ("The mere fact that the prior art could be so modified would not have made the

modification obvious unless the prior art suggested the desirability of the modification.") Because He et al. fails to disclose or provide any motivation for collecting security information from a user contemporaneously with the initiation of a function within a process control system, it follows that He et al. cannot render any of the claims at issue obvious.

In fact, He et al. does not recognize that its system contains the very security problem which the claimed system solves, i.e., the problem of an unauthorized user gaining access to an unattended machine after a login procedure has been performed on that machine by an authorized user. Thus, while the He et al. system may prevent unauthorized access using another machine, He et al. does not address or even recognize the problem of an unauthorized user gaining access to an unattended but authorized machine after a login procedure has been performed at that machine, much less suggest a manner of solving this problem. Moreover, He et al. actually teaches away from the claimed system and method, as He et al. sets up a procedure (i.e., the use of a session ticket) that is designed to reduce the number of times the user has to supply user security information, not one that requires the user to do so upon initiating a function (as required by the pending claims), which generally increases the number of times that a user has to supply security information. For this further reason, He et al. cannot render any of the pending claims obvious.

CONCLUSION

For the foregoing reasons, applicants respectfully request reconsideration and withdrawal of the rejections and allowance of claims 1-18, 20-29, and 32. If there are matters that can be discussed by telephone to further the prosecution of this application, applicants respectfully request the examiner to call its attorney at the number listed below.

Respectfully submitted,

By: 

Roger A. Heppermann
Registration No. 37,641
MARSHALL, GERSTEIN & BORUN LLP
6300 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6402
312-474-6300

May 24, 2005